BY ORDER OF THE COMMANDER
302D AIRLIFT WING

302 AIRLIFT WING INSTRUCTION 31-401

19 JUNE 2014

Security

302D AIRLIFT WING SECURITY PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this instruction. This instruction may be released to DoD civilian, contractors, and military members assigned to the 302 AW. Refer other requests for this document to 302 AW/PA.

OPR: 302 AW/SFO

Certified by: 302 AW/CC
(Col Jack H. Pittman, Jr.)

Pages: 14

Supersedes: 302AWI31-401,
3 February 2007

This instruction implements DoD Manual 5200.01, *DoD Information Security Manual*, Volumes 1-4, Air Force Instruction (AFI) 31-401, *Information Security Program Management*, AFI31-406, *Applying North Atlantic Treaty Organization (NATO) Protection Standards*, AFI31-501, *Personnel Security Program Management*, AFI31-601, *Industrial Security Program Management*, and AFI16-701, *Special Access Program*. It establishes policies and procedures governing the security program within the 302d Airlift Wing (AW). It defines individual roles in program management and assigns specific responsibilities to functional managers. The program is designed to provide increased security awareness and education to all personnel responsible for safeguarding Air Force operations and sensitive national defense information at all times and under all circumstances. It applies to all military, civilian, and contractor personnel assigned to the 302d Airlift Wing. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) or any updated statement provided by the AF Records Management office (SAF/CIO A6P). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command.

SUMMARY OF CHANGES

This instruction has been substantially revised to reflect updates referenced in AFI 31-401 and DoDM 5200.01,Volumes 1-4, Change 2. SAF/AAZ officially instructed implementation of all 4 volumes of DoDM 5200.01 as included in AFGM2 to AFI 31-401. Revisions made to this instruction redefine, clarify and outline roles and responsibilities for security operations within 302 AW.

1. Background/Overview. This Air Wing Instruction (AWI) serves as an overall 302 AW procedure for Security operations. The goal of this program is to comply with regulations and produce an effective wing security plan. This AWI does not contain all Information Security guidance but rather is a conduit for general Security Operations. For complete Security guidance refer to the Glossary of References at the end of this AWI

2. Policy. It is 302 AW policy to train and assist personnel on how to identify, safeguard, store, transmit, derive, downgrade, declassify, mark, reproduce, and destroy classified information and material consistent with national policy. This general policy statement also applies to unclassified controlled information under the purview of relevant statutes, regulations, instructions, and directives.

3. Responsibilities, Authorities, and Accountability.

3.1. Each group, squadron, and detachment commander will appoint in writing a primary and alternate unit security manager (USM), to ensure compliance with security directives for the protection of classified material. The original memorandum of appointment will be sent to the 302d Security Forces Squadron Information Security staff. This memorandum will help identify a single point of contact within each organization for security matters.

3.1.1. Ensure primary and alternate unit security managers receive training for their assigned security programs and duties within 90 days of appointment in accordance with (IAW) AFI31-401.

3.1.2. Delegate, via appointment letter, NATO access granting authority to the unit security managers.

3.1.3. Designate, in writing, equipment and personnel approved for classified reproduction.

3.1.4. Follow security incident provision in paragraph 2.8 when appropriate.

3.2. Wing Security Manager Responsibilities. Review and update this instruction every four years.

3.3. Unit Security Manager Duties for Information Security, Personnel Security and Industrial Security Programs.

3.3.1. The Unit Security Manager will personally implement and oversee all elements of an effective security program addressing Information, Personnel, Industrial, resources security working directly with the 21SW/IP office for guidance and oversight.

3.3.2. Provide advice and assistance to the commanders and unit personnel on security related issues and ensure compliance with security directives.

3.3.3. Ensure a copy of the wing instruction for security guidance is implemented and followed, and electronic or hard copies of applicable instructions, as stated in introduction paragraph of this instruction, are accessible.

3.3.4. Ensure unit personnel receive initial and annual refresher training IAW AFI31-401.

3.3.5. Conduct semi annual internal self-inspections IAW 21SW/IP Peterson AFB Security Manager Self Inspection Guide checklists.

3.3.6. Attend scheduled security manager's meetings or ensure a unit representative attends.

3.3.7. Assist and provide guidance to those involved in security incidents (i.e, inquiry/ investigating official, and appointing authority). Monitor security incidents from initiation to closing, ensuring the timely reporting of the incident and submission of reports.

3.3.8. Develop local Emergency Protection Plan for classified with unit commanders and post in classified working and storage areas.

3.3.9. Ensure each Commanders Support Staff / Mail handlers are aware of provision of **paragraph 2.2.6** of this instruction.

3.3.10. Assist Unit Security Managers with base coordination updating security clearances.

3.3.11. Coordinate change requests to the Unit Manning Document (UMD) relating to Security Access Requirement (SAR CODE).

3.3.12. Brief personnel and maintain AF IMT 2583 in the security manager’s files on each individual requiring NATO access. Individuals must be debriefed by the unit security manager by completing the AF IMT 2587, Security Termination Statement, when access is no longer needed (i.e., permanent change of station (PCS)/ permanent change of assignment (PCA)/temporary duty (TDY) 90 days or more).

3.3.13. Complete AF IMT 2587 for every military or civilian member retiring or separating from the service. Additionally, civilian employees with special access terminating employment for more than 60 days need to complete AF IMT 2587.

3.3.14. Issue Courier Authorization Letters.

3.3.15. Maintain documentation identified in self inspection checklist.

3.3.16. Ensure this program governs the protection of classified defense information in the hands of government contractors doing business with the government.

3.3.17. Request and receive Joint Personnel Adjudication System (JPAS) visit authorization requests for all industrial contractors working within the unit and provide clearance verifications.

3.3.18. Maintain liaison with all contractors, field representatives and the base industrial security personnel providing security support as required.

3.3.19. Maintain a security manager’s handbook.

3.4. Security incident investigator responsibilities are briefed by the 21SW/IP office.

3.4.1. Ensure investigator attends training, writes investigation report IAW **paragraph 2.8**, brief commander (CC); forwards report to 21SW/IP.

4. Procedures.

4.1. Storage, handling, and transmission of classified material. Classified material will be received, handled, stored, and transmitted IAW DoD 5200.1-R and AFI31-401. 21SW/IP will provide guidance and approval for all vault and secure room approval.

4.1.1. Security Containers/Vaults/Sensitive Compartmented Information Facility (SCIF)s.

4.1.1.1. Incoming classified material will be stored in a General Services Administration (GSA) approved security container, secure room or a Class A/B vault or vault type room that meets the standards established by the head of the DoD Component concerned.

4.1.1.2. Every security container must have a primary and alternate safe custodian appointed in writing and forwarded to the unit security manager.

4.1.1.3. All security containers must be assigned an identification number.

4.1.1.4. Security containers/vault custodians must insure inspections of the container IAW Technical Order (TO) 00-20F-2, Inspection and Preventive Maintenance Procedures for Classified Storage Containers, to ensure it is authorized for storage of classified. Document the inspection on an Air Force Technical Order (AFTO) IMT 36, Maintenance Record for Security Type Equipment. Only GSA certified locksmiths may accomplish a Preventive Maintenance Inspection (PMI). Security containers and secure rooms are required to be inspected every 2 years and vaults every 5 years.

4.1.1.5. Personnel opening/closing containers/vaults or secure rooms will use the Standard Form (SF) 702, Security Container Check Sheet**.** If evidence of tampering is identified and the container has Communication Security (COMSEC) material, the COMSEC custodian will be notified. If Sensitive Compartmented Information (SCI) material is involved, the local Special Security Office (SSO) will be notified. For all other incident related occurrences contact the 21SW/IP office.

4.1.1.6. Unescorted access to a secure room will be controlled and limited to personnel cleared for access. Additionally, personnel must have a need-to-know to perform official duties. Positive identification will be made for an individual requesting access. If the individual is not cleared, but has a valid reason for entry, the area will be sanitized and personnel within the area will be made aware of their presence. To sanitize the area before un-cleared personnel enter, remove all classified material from immediate or open view and do not discuss classified information.

4.1.1.7. Each individual authorized access to any secure room is responsible for knowing and understanding procedures for accessing and securing these areas. Once opened, the vault or secure room must be manned at all times or be secured. Each secure room will maintain a Security Instruction. This instruction should be

reviewed annually for all personnel working in the area or identified on the Entry Authorization List (EAL).

4.1.1.8. Combinations to containers/vaults/secure rooms will be given only to those personnel requiring access on a regular basis. Custodians will notify authorized personnel of changes. The stored combination will be kept in a sealed Standard Form (SF) 700, Security Container Information Form, and marked with the appropriate office symbol, safe number, and stamped with the highest classification stored within the container/secure room.

4.1.1.9. Combinations to containers/vaults/secure rooms will be changed when approved personnel PCS, PCA, separate, retire, a compromise has occurred, or when an individual no longer require access, when maintenance is performed, or at least annually if the container or secure room contains NATO Secret material.

4.1.1.10. Resource Modification/Relocation. When physical security properties of the secure room (i.e., floors, walls, ceilings, doors, etc.,) are modified or when resources being protected are relocated, 21SW/IP must have prior notification, in writing.

4.2. **Handling.**

4.2.1. Individuals are authorized to review, handle, receive and process classified information equal only up to their clearance level.

4.2.2. All personnel who handle or process classified material are responsible for providing protection and accountability for the material at all times. Always keep classified material under your control and protect documents with cover sheets.

4.2.3. All computer products created on accredited systems will be classified at their appropriate security level until reclassified or declassified by the Original Classification Authority (OCA). Products will be accounted for, controlled, marked and protected in accordance with the assigned classification. Working papers containing classified information shall be dated when created and annotated with the organization, office symbol, and phone number of the originator. Working papers will be destroyed when no longer needed or when the document is 180 days old.

4.2.4. Magnetic media will be marked, stored and handled IAW AFI31-401, chapter 4.

4.2.5. When loaning out classified material within or outside the organization, use an AF Form 614, Charge Out Record or an AF Form 310, to establish a suspense for returning material.

4.2.6. All registered mail will be treated and protected as classified until the classification of the contents can be verified.

4.2.7. Classified material will not be taken to an individual's private residence or temporary quarters.

4.2.8. Marking "Derivatively Classified" Documents. Derivative classification is the act of incorporating, paraphrasing, restating, or generating in new form, information that is already classified, and marking the newly developed material consistent with the markings of the source information. As with documents created by original classifiers,

each derivative document must have portion markings and overall classification markings. Identify the source used as the basis for classification on the "Derived from" line of the derivative document. The "Declassify on" line of the source document is carried forward to the "Declassify on" line of the derivative document.

4.3. **Reproducing classified material.** Classified reproduction should be kept to the minimum required to accomplish the mission. All copies are subject to the same controls and safeguards as the original document. Contact unit security manager for additional guidance.

4.3.1. Portions of documents and materials that contain Top Secret information shall not be reproduced without the consent of the originator or higher authority. Record the number of copies reproduced and the identity of each recipient on the original document. The Office of Primary Responsibility (OPR) must be notified when copies are destroyed.

4.3.2. Equipment identified for classified reproduction must be approved by the 21SW/IP.

4.3.3. Marking Equipment. The following statement should be posted when copier has been approved for classified reproduction: "THIS EQUIPMENT AUTHORIZED FOR REPRODUCTION OF CLASSIFIED MATERIAL". The following statement should be posted when the copier has NOT been approved for classified reproduction: "STOP, DO NOT USE THIS MACHINE FOR CLASSIFIED REPRODUCTION".

4.4. **Hand-carrying Classified Material.** Classified material may be removed from the unit only in the performance of official duties. The provisions of DoD 5200.1-R/AFI31-401, chapter 6, apply for transmitting/transporting classified information. Individuals authorized to hand-carry classified material shall be fully briefed of these provisions. Whenever classified information is transported outside the work area, it shall be enclosed in a sealed envelope, double wrapped folder, or other closed container (locked briefcase) to prevent loss or observation. Furthermore, you must have official written authorizations signed by the commander: a Designation of Official Courier Memorandum and an Exemption Notice (both the memorandum and the exemption notice must be in English and the language of any country the personnel will have opportunity to enter; i.e., Poland or France for temporary duty (TDY) purposes). Additionally, consideration must be given to mode of transportation, time sensitivity, authorized storage availability at the destination, transfer or accountability at destination, or method of returning material. Contact the security office for instructions. Use the following guidance for hand-carrying classified material:

4.4.1. On Base, with no entry/exit inspection points. Verbal authorization from the unit commander is required for hand-carrying classified information between buildings or areas within the confines of the installation.

4.4.2. On base, with entry/exit inspection points. Verbal authorization from the unit commander is required for hand-carrying classified information between buildings or areas within the confines of the installation.

4.4.3. Outside your duty location. When hand-carrying any classified information outside the confines of your duty location you must have an official courier memorandum, and an exemption notice.

4.4.4. Commercial. Hand-carrying classified material on a commercial aircraft will not be done unless under emergency situations. All requirements to carry on commercial aircraft must be approved by the Wing commander, providing all requirements are met IAW AFI31-501, DOD 5200.1-R, paragraph **7-302(e)**. If travel involves passage through an inspection point where classified may be subject to examination by non-DoD personnel or involves overnight stopovers, contact the unit security manager for proper procedures.

4.5. **Mailing.**

4.5.1. Secret. The AF IMT 310, Document Receipt and Destruction Certificate, is required. Contact unit security manager for proper procedures.

4.5.2. Confidential. The AF IMT 310, Document Receipt and Destruction Certificate, is required. Contact unit security manager for proper procedures.

4.6. **Foreign Travel Policy.**

4.6.1. Each unit member is responsible for maintaining a list of their foreign travel. This information will be used when completing clearance updates.

4.6.2. Members who have access to SCI information must submit any anticipated leisure travel to foreign countries to the unit security manager, or report any travels within 3-days upon return. The security manager will ensure personnel receive proper briefings if threat conditions exist in the areas of travel. Individuals will report contacts of a suspicious nature to their supervisor, security manager or local OSI upon return.

4.7. **Disposal of Classified.**

4.7.1. Classified material will be destroyed as soon as it has served its purpose and shall be destroyed by an NSA approved crosscut shredder. Destruction of classified material and documentation of destruction will be accomplished as follows:

4.7.1.1. Top Secret. Two people with appropriate clearance must be present and a destruction certificate must be completed. Use the AF IMT 143, with two signatures and maintain in accordance with the records disposition schedule in **https://afrims.amc.af.mil**.

4.7.1.2. Secret and Confidential. IAW AFI31-401, paragraph 5.29.2.2. A record of destruction is not required but an appropriately cleared person must be involved in the destruction process. No destruction certificate is required. Maintain in accordance with the records disposition schedule in **https://afrims.amc.af.mil**.

4.7.1.3. IAW AFI31-406, paragraph 5.12.2. NATO Secret requires a destruction certificate with two signatures. AF IMT 310 can be used for the destruction certificate. File destruction certificate in IAW AFMAN 37-139. Maintain in accordance with the records disposition schedule in **https://afrims.amc.af.mil**.

4.7.2. Classified magnetic media will be properly protected and stored until degaussed. Destruction records are not required.

4.7.3. Annual Clean-Out Day. The unit training assembly (UTA) of June is the wing clean-out day. IAW AFI31-401 this day is designated to purge and maintain in

accordance with the records disposition schedule in **https://afrims.amc.af.mil**. Normal documentation is required.

4.7.4. Emergency destruction or relocation of classified material will be done by personnel IAW Emergency Protection Plans for the vault, container or secure room which holds the classified material.

4.7.4.1. Procedures for Non-hostile Emergencies.

4.7.4.1.1. Time and circumstances permitting immediately return classified material to its storage container and secure it.

4.7.4.1.2. If immediate evacuation of the area is required (fire, bomb threat, etc.), take any classified material you have with you when departing. Then contact your supervisor for assistance in securing it. At no time, risk your life or safety to protect classified material. If there is too much to remove, to secure safely or quickly, leave it. Personnel who have been trained and pre-instructed to prevent the removal of classified material will be placed around the affected area to protected classified materials and reduce casualty risk. When you're safe, notify your supervisor or commander of the location of the material.

4.7.4.1.3. If it is anticipated that classified material would be jeopardized if left in place, and there is sufficient time, take it to the Base Command Post, 21st Mission Support Squadron, Director of Information management (21 MSS/MSI), Building 862 for safekeeping. The 21st Communications Squadron (CS), Building 1038, is an alternate location. If you need to move an entire storage container, contact Security Forces to obtain a secure area.

4.7.4.2. Procedures for Hostile Emergencies. The installation commander or senior on-scene commander will decide whether to move materials to vaults, remove materials from vaults, remove materials from the installation, or destroy all classified materials.

4.7.4.2.1. Storage vaults are located in the Base Post Office, building 1460.

4.7.4.2.2. Evacuation of materials will be by ground movement to the North American Aerospace Defense Command (NORAD)/Cheyenne Mountain Complex (NCMC) tunnel or by air movement as directed by the commander. Use escorts, marshalling area guards, etc. as directed.

4.7.4.2.3. Approved methods of destruction are by NSA approved crosscut shredding.

4.7.4.2.3.1. Destruction of top secret information must be witnessed by 2 appropriately cleared personnel and documentation is required for the destruction. Documentation must be completed on an AF IMT 310.

4.7.4.2.3.2. Primary Emergency Method. Time permitting; take materials to the Base Destruction Facility, building 600. This facility is controlled by 21 MSS/MSI, building 862.

4.7.4.2.3.3. Alternate emergency method. Use only if the base facility is not available in time to be used. Burn classified documents at the southwest end

of building 895 using metal trashcans or other suitable containers. Separate and crumple pages before burning, and insure complete destruction before leaving area. If other approved methods of destruction are available they may be used in lieu of burning. However, the destruction personnel must ensure the information is properly destroyed before departing the area.

4.7.4.2.4. Procedures for COMSEC material. Refer to DOD 5200.1-R and AFI31-401, chapter 5 for procedures used to report any mission, compromised, or destroyed classified material.

4.8. **Security Incidents.** A security incident may result in damage to our national security. Security incidents are normally caused by a violation of established procedures for handling, storing, transferring, or accounting of classified information. In the event of a violation and the material discovered is classified, secure it immediately and report the incident to the supervisor, security manager or commander.

4.8.1. Conducting inquiries or investigations. A preliminary inquiry is conducted whenever a security incident involving classified information occurs. The categories of security incidents are:

4.8.1.1. COMPROMISE: The disclosure of classified information to persons not authorized.

4.8.1.2. POTENTIAL COMPROMISE: When an investigating official concludes that a compromise probably occurred as a result of the security incident.

4.8.1.3. SECURITY INFRACTION: An incident that involves the misuse or improper handling of classified material, but does not fall into the categories of compromise, probable compromise, or inadvertent access.

4.8.2. Once the group/squadron or detachment commander gains knowledge of a security incident, he/she is responsible for initiating a preliminary inquiry under DoD 5200.1-R and AFI31-401, chapter 9. The commander will ensure:

4.8.2.1. The incident is reported to 21SW/IP within one duty day.

4.8.2.2. A preliminary inquiry officer (IO) is appointed in writing. Security managers will not be appointed. A field grade officer, MSgt, or general schedule (GS)-09 or above will be appointed. Individuals appointed should be of a higher grade than the person suspected of causing the incident. The individual appointed should not be from the same office in which the incident occurred.

4.8.2.3. The report will be completed within 10 duty days from the date of appointment or request an extension in writing and must be submitted to the commander.

4.8.3. Duties of the preliminary inquiry officer.

4.8.3.1. The IO must contact 21SW/IP for a briefing for technical guidance in conducting the inquiry.

4.8.3.2. Consider the circumstances surrounding the incident and assign a category for the incident.

4.8.3.3. Question personnel involved. Identify person(s), acts, conditions which caused the incident.

4.8.3.4. Complete report and have the security manager review the report. The investigating officer then forwards the report to 21SW/IP.

4.8.4. Duties of the security manager for security incidents.

4.8.4.1. Assist and provide guidance to those involved in the security incident (i.e., inquiry/investigation official and appointing authority).

4.8.4.2. Be familiar with directives concerning security incidents.

4.8.4.3. Ensure security incidents are reported to the 21SW/IP within one duty day of discovery.

4.8.4.4. Monitor security incident from appointment to closing.

4.9. **Security Awareness.** A good security education program is the key to attaining a solid security program. It is imperative training be taken seriously and be accomplished in a manner that stresses the importance of security.

4.9.1. Each unit security manager will ensure all military, GS civilians, and contractors receive the required quarterly security awareness training IAW AFI31-401, chapter 7.

4.9.2. Supervisors will verify newcomer's security clearances through the unit security manager prior to allowing them to perform any function involving access to classified information. Supervisors will brief all incoming personnel on security requirements and practices within their work center. Supervisors will ensure all newcomers report to the unit security manager within 30 duty days of arrival for security in-processing.

4.10. **Security Inspections.** Security self-inspections will be conducted on a semi-annual basis. The self-inspection official will be appointed in writing by the commander. Security managers will not inspect their own programs.

4.10.1. Forward inspection results in memorandum format, endorsed by the commander to the unit security manager. Security manager will follow-up on any items needing correction or completion.

4.11. **End of Day Procedures.** End-of-day security checks must be documented on a SF 701, Activity Security Checklist. Each work area shall establish that the last person leaving the work area will ensure all items listed on the SF 701 are checked and signed off. The SF 701 should be posted near the exit of the room being checked.

4.11.1. Checks should include rooms and areas where classified material can be viewed, stored, processed, copied, printed or faxed to ensure all material is properly removed and secured.

4.11.2. Ensure individuals with at least a Secret clearance perform end-of-day checks and lockup if classified in the area.

4.11.3. If the work center has security containers (safes, vault doors, open storage areas) include them on the SF 701 checklist to ensure they are secured. Ensure all windows and doors are locked and all appliances are turned off. All personnel must check their desk

and surrounding area for classified material that may have inadvertently been discarded or misplaced during the day.

4.11.4. Individuals working or entering the facility after normal duty hours perform another end of day check prior to leaving the facility. This check will also be annotated on the SF 701.

4.12. **Secure Telephone Equipment (STE) cards.**

4.12.1. The terminal is treated as an unclassified, high value item when the Crypto Ignition Key (CIK)/STE card is not inserted. When a CIK/card is inserted into the terminal, the unit must not be left unattended. Unless the STE is located in an area operational 24-hours a day, the CIK/card must be removed and properly secured at the close of each business day.

4.12.2. Storage of CIK/STE. IAW AFI AFI33-201V9, Operational Instructions For Secure Voice Devices, when the key is stored in the same room as the terminal, store the CIK/card in a GSA-approved security container. If a security container is not available store the CIK/card in a locked cabinet or desk, provided the door to the room containing the STE is locked.

JACK H. PITTMAN, JR., Col, USAFR
Commander

Attachment 1

GLOSSARY OF REFERENCES, ACRONYMNS, AND DEFINITIONS

References

DoD 5200.1-R, *Information Security Program*

DoDM 5200.01, Implementation memorandum, DoD Information Security Program

DoDM 5200.01, Vol 1, Overview, Classification, and Declassification

DoDM 5200.01, Vol 2, Marking of Classified Information

DoDM 5200.01, Vol 3, Protection of Classified Information

DoDM 5200.01, Vol 4, Controlled Unclassified Information (CUI)

AFI 16-701, *Special Access Program*

AFI31-401, *Information Security Program Management*

AFI 31-406, *Applying Treaty Organization (NATO) Protection Standards*

AFI 31-501, *Personnel Security Program Management*

AFI 31-601, *Industrial Security Program Management*

AFI AFI33-201V9, *Operational Instructions For Secure Voice Devices*

TO 00-20F-2, *Inspection and Preventive Maintenance Procedures for Classified Storage Containers*

Forms/IMT Adopted

AF IMT 2583, **Request for Personnel Security Action**

AF IMT 2587, **Security Termination Statement**

AF Form 614, **Charge Out Record**

AF IMT 310, **Document Receipt and Destruction Certificate**

AF IMT 143, **Top Secret Register Page**

AF IMT 1565, **Entry, Receipt and Destruction Certificate**

AFTO IMT 36, **Maintenance Record for Security Type Equipment**

DD Form 1879, **Security Investigation, DOD Request For Personnel**

SF 700, **Security Container Information Form**

SF 701, **Activity Security Checklist**.

SF 702, **Security Container Check Sheet**

Acronyms

AF—Air Force

AFGM2—Air Force Guidance Memorandum 2

AFI—Air Force Instructions

AFOSI—Air Force Office of Special Investigations

AFTO—Air Force Technical Order

ASCAS—Automated Security Clearance Approval System

AW—Airlift Wing

CC—Commander

CF—Communications Flight

CIK—Crypto Ignition Key

COMSEC—Communications Security

CS—Communications Squadron

DD—Department of Defense

DoD—Department of Defense

DoDM—Department of Defense Manual

DoDSI—Department of Defense Security Institute

EPSQ—Electronic Personnel Security Questionnaire

GS—General Schedule

GSA—General Services Administration

IAW—In Accordance With

IMT—Information Management Tool

IO—Inquiry Officer

ISPM—Security Program Manager

JPAS—Joint Personnel Adjudication System

MSI—Director of Information management

MSS—Mission Support Squadron

NATO—North Atlantic Treaty Organization

NCMC—North American Aerospace Defense Command/Cheyenne Mountain Complex

NORAD—North American Aerospace Defense Command

NET—Network

OCA—Original Classification Authority

OPR—Office of Primary Responsibility

PCA—Permanent Change of Assignment

PCS—Permanent Change of Station

SCIF—Sensitive Compartmented Information Facility

SC—Superintendent

SCI—Sensitive Compartmented Information

SAR CODE—Security Access Requirement

SF—Standard Form

SFAI—Information Security Staff

SFS—Security Forces Squadron

SPACLAN—Space Command Local Area Network

SCO—Special Security Office

STE—Secure Telephone Equipment

TDY—Temporary Duty

TO—Technical Order

UMD—Unit Manning Document

USM—Unit Security Managers

UTA—Unit Training Assembly

Terms

COMPROMISE—The disclosure of classified information to persons not authorized.

POTENTIAL COMPROMISE—When an investigating official concludes that a compromise probably occurred as a result of the security incident.

SECURITY INFRACTION—An incident that involves the misuse or improper handling of classified material, but does not fall into the categories of compromise, probable compromise, or inadvertent access.